(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－358283
（P2002－358283A）
(43)公開日　平成14年12月13日(2002.12.13)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ	５Ｊ１０４

審査請求　有　　請求項の数26　ＯＬ　（全 16 頁）

(21)出願番号　特願2001－166114(P2001－166114)

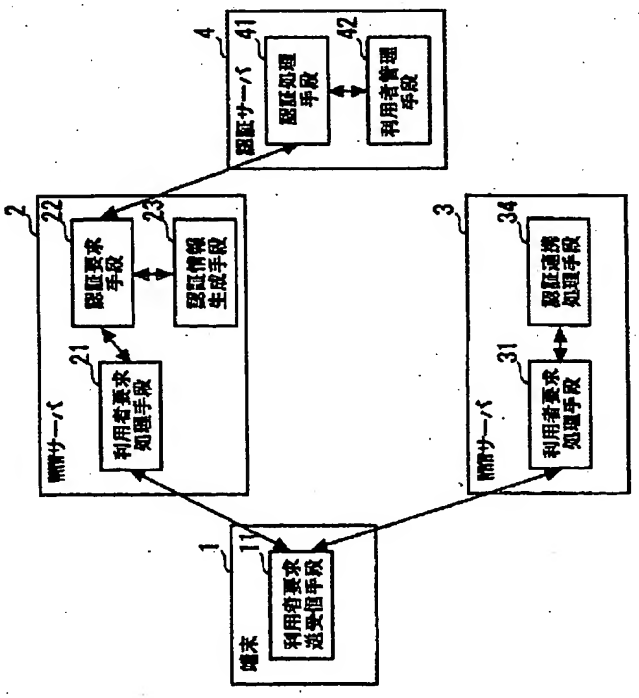
(22)出願日　平成13年６月１日(2001.6.1)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　田中　広幸
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100080816
弁理士　加藤　朝道

Ｆターム(参考)　5B085 AC12 AE02 AE23 BG07
5J104 AA07 MA04 PA07

(54)【発明の名称】　利用者認証連携方法とシステム及びプログラム

(57)【要約】
【課題】認証を行うサーバを利用できないＷＷＷサーバでも、認証の連携を可能とする利用者認証連携システム及び方法の提供。
【解決手段】ＷＷＷサーバ２は、端末１が、利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を認証サーバ４に送信する手段２１、２２と、認証サーバでの認証が成功した場合に、前記利用者の前記利用者情報と時間情報から認証情報の生成する認証情報生成手段２３と、前記生成された認証情報を、要求結果と共に、前記端末に送信する手段２１と、を備え、端末１は、ＷＷＷサーバ３に要求を送信する場合、認証情報を送信し、ＷＷＷサーバ３は認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段３４と、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段３１とを備える。



1

【特許請求の範囲】

【請求項１】端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から送信された利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、

前記一の情報提供サーバが、生成した前記認証情報を、前記端末に送信するステップと、

前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報から、利用者情報と時間情報を取り出して、認証判定を行うステップと、

を含む、ことを特徴とする利用者認証連携方法。

【請求項２】前記一の情報提供サーバは、前記端末から前記一の情報提供サーバに送信された前記利用者情報を、前記一の情報提供サーバに接続する認証サーバに送信するステップを実行し、前記認証サーバで認証が正しく行われた場合に、前記認証サーバでの認証結果を受けた前記一の情報提供サーバにおいて、前記認証情報を生成するステップと、前記認証情報を前記端末に送信するステップと、が実行される、ことを特徴とする請求項１記載の利用者認証連携方法。

【請求項３】前記認証判定を行うステップで、認証が成功した場合、認証の連携処理を行う前記情報提供サーバでは、前記認証情報から前記利用者情報を取り出し、前記利用者情報と時間情報とから、あらたに認証情報を生成し、前記端末に、あらたに生成された前記認証情報を送信するステップを含む、ことを特徴とする請求項１記載の利用者認証連携方法。

【請求項４】あらたに生成された前記認証情報を受信した前記端末が、認証の連携処理を行う情報提供サーバに要求を送信する場合に、前記認証情報を、認証の連携処理を行う前記情報提供サーバに送信するステップと、

認証の連携処理を行う前記情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、前記認証情報から利用者情報と時間情報を取り出して、認証判定を行い、認証が成功した場合、前記認証情報から取り出された前記利用者情報と、時間情報から、あらたに認証情報を生成し、前記端末に、あらたに生成された前記認証情報を送信するステップと、

を含む、ことを特徴とする請求項３記載の利用者認証連携方法。

【請求項５】前記認証情報の生成に用いられる前記時間情報が、前記認証情報を生成する情報提供サーバのシステム時計の時間情報である、ことを特徴とする請求項１乃至４のいずれか一に記載の利用者認証連携方法。

【請求項６】端末が、利用者からの要求と、利用者認証を行うための利用者情報を、一の情報提供サーバに送信するステップと、

前記一の情報提供サーバでは、前記利用者情報を、前記

2

一の情報提供サーバが接続する認証サーバに送信し、前記認証サーバでの認証が成功した場合に、前記一の情報提供サーバの認証情報生成部にて、認証情報を生成するステップと、

前記一の情報提供サーバは、前記一の情報提供サーバの前記認証情報生成部で生成された前記認証情報を、要求結果と共に、前記端末に送信するステップと、

前記端末が、前記一の情報提供サーバと連携し、認証の連携処理を行う他の情報提供サーバに要求を送信する場合、前記要求とともに、前記認証情報を、前記他の情報提供サーバを送信するステップと、

前記他の情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、認証連携処理部で、受け取った前記認証情報を基に、認証の連携処理を行うステップと、

前記他の情報提供サーバにおいて、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信するステップと、

を有する、ことを特徴とする利用者認証連携方法。

【請求項７】前記認証情報生成部で生成される認証情報が、利用者情報と時間情報と、チェックデータとを含み、これらの情報が暗号化されている、ことを特徴とする請求項６記載の利用者認証連携方法。

【請求項８】前記認証連携処理部で認証の連携処理を行うステップが、

受け取った前記認証情報を復号するステップと、

復号された前記認証情報のチェックデータを検査するステップと、

前記チェックデータの検査が成功した場合、復号された前記認証情報から利用者情報と時間情報を取り出すステップと、

前記取り出された時間情報に基づき時間の検査を行うステップと、

前記時間検査が成功した場合、認証成功とするステップと、

を含む、ことを特徴とする請求項６又は７記載の利用者認証連携方法。

【請求項９】利用者からの要求に対し、最初の情報提供サーバへのアクセスの場合、前記認証サーバを利用した利用者認証処理を行い、

続く情報提供サーバへのアクセスでは情報提供サーバでの認証連携処理を行う、ことを特徴とする請求項６又は７記載の利用者認証連携方法。

【請求項１０】前記一の情報提供サーバが認証の認証連携を行う認証連携処理部を有し、

前記一の情報提供サーバでは、前記端末から送信された認証情報を受け取り、前記認証連携処理部で認証の連携処理を行い、認証判定が成功した場合、前記一の情報提

供サーバの認証情報生成部に認証情報の生成を依頼するステップと、

前記一の情報提供サーバの前記認証情報生成部は、前記一の情報提供サーバの前記認証連携処理部が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、

を含む、ことを特徴とする請求項６記載の利用者認証連携方法。

【請求項１１】認証の連携処理を行う前記他の情報提供サーバが認証情報生成部を有し、

前記他の情報提供サーバの認証連携処理部で認証の連携処理を行い、認証判定が成功した場合、前記他の情報提供サーバの認証情報生成部に認証情報の生成を依頼するステップと、

前記他の情報提供サーバの認証情報生成部は、前記認証連携処理部が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、

前記他の情報提供サーバが、利用者の要求結果と、生成した前記認証情報を前記端末に送信するステップと、

を含む、ことを特徴とする請求項６又は１０記載の利用者認証連携方法。

【請求項１２】端末からネットワークを介してアクセスされる一の情報提供サーバが、

前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから認証情報を生成し、生成した前記認証情報を、前記端末に送信する手段を備え、

前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行う手段を備えている、ことを特徴とする利用者認証連携システム。

【請求項１３】端末と、該端末からネットワークを介してアクセスされる複数の情報提供サーバと、を有し、

前記複数の情報提供サーバには、認証サーバに接続される少なくとも一つの情報提供サーバと、認証の連携処理を行う少なくとも一つの情報提供サーバと、が含まれ、

前記認証サーバに接続される一の情報提供サーバは、前記端末が、利用者からの要求と、利用者認証を行うための利用者情報を、前記一の情報提供サーバに送信した場合、これを受信し、前記利用者情報を、前記認証サーバに送信する手段と、

前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成手段と、

前記生成された認証情報を、要求結果と共に、前記端末に送信する手段と、

を備え、

前記端末は、認証の連携処理を行う前記情報提供サーバに要求を送信する場合、前記一の情報提供サーバより送信された前記認証情報を、認証の連携処理を行う前記情報提供サーバに送信する手段を備え、

認証の連携処理を行う前記情報提供サーバは、前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段と、

前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段とを備えている、ことを特徴とする利用者認証連携システム。

【請求項１４】前記一の情報提供サーバの前記認証情報生成手段が、前記利用者情報と、時間情報と、チェックデータとからなる情報を暗号化したものを、前記認証情報として出力する、ことを特徴とする請求項１３記載の利用者認証連携システム。

【請求項１５】利用者からの要求に対し、最初の情報提供サーバへのアクセスの場合、前記認証サーバを利用した利用者認証処理を行い、続くアクセスでは、情報提供サーバの認証連携処理を行うことを特徴とする請求項１３記載の利用者認証連携システム。

【請求項１６】前記一の情報提供サーバが、

前記端末からの利用者の要求を処理する利用者要求処理手段と、

前記認証サーバに対して認証要求を行い、前記認証サーバで認証が成功した場合、認証情報を生成するように要求する認証要求手段と、

を備え、

前記認証情報生成手段は、前記認証要求手段からの要求を受けて、前記利用者情報と時間情報とから前記認証情報を生成し、

前記利用者要求処理手段は、前記端末に対して、要求結果と、前記生成された認証情報とを送信する、ことを特徴とする請求項１３記載の利用者認証連携システム。

【請求項１７】認証の連携処理を行う前記情報提供サーバが、

前記端末からの利用者の要求を処理する利用者要求処理手段を備え、

前記認証連携処理手段が、前記端末から要求とともに送信される認証情報を受け取り、前記認証情報を基に、認証の連携処理を行い、

前記認証連携処理手段での認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者要求処理手段では、前記利用者の要求を受け付け、要求結果と共に、新たに生成された前記認証情報を、前記端末に送信する、ことを特徴とする請求項１３記載の利用者認証連携システム。

【請求項１８】前記認証連携処理手段が、

前記認証情報を復号する手段と、

5

復号された前記認証情報のチェックデータを検査する手段と、
前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す手段と、
前記時間情報の検査を行う手段と、
を含み、前記時間情報の検査結果が正しい場合、認証成功とする、ことを特徴とする請求項１３記載の利用者認証連携システム。
【請求項１９】前記一の情報提供サーバが、認証連携処理手段をさらに備え、
前記一の情報提供サーバは、前記端末から送信された認証情報を受け取り、前記一の情報提供サーバの前記認証連携処理手段で認証連携を行い、認証判定が成功した場合、前記一の情報提供サーバの前記認証情報生成手段に対して認証情報の生成を依頼し、
前記一の情報提供サーバの前記認証情報生成手段は、前記認証連携処理手段が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報から認証情報を生成する、ことを特徴とする請求項１３記載の利用者認証連携システム。
【請求項２０】認証の連携処理を行う前記情報提供サーバが、認証情報生成手段を備え、
認証の連携処理を行う前記情報提供サーバが、前記認証連携処理手段で認証連携を行い、認証判定が成功した場合、認証の連携処理を行う前記情報提供サーバの前記認証情報生成手段に認証情報の生成を依頼し、
認証の連携処理を行う前記情報提供サーバの前記認証情報生成手段が、前記認証連携処理手段が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報とから認証情報を生成し、利用者の要求結果と前記認証情報を前記端末に送信する、ことを特徴とする請求項１３又は１９記載の利用者認証連携システム。
【請求項２１】端末からネットワークを介してアクセスされる一の情報提供サーバが、
（ａ）前記端末から利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する処理と、
（ｂ）前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成処理と、
（ｃ）前記生成された認証情報を、要求結果と共に、前記端末に送信する処理と、
を有し、
端末からネットワークを介してアクセスされ前記一の情報提供サーバと認証の連携処理を行う情報提供サーバが、
（ｄ）前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理と、

6

（ｅ）前記認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する処理とを含み、
前記各処理を前記各情報提供サーバで実行させるためのプログラム。
【請求項２２】請求項２１記載のプログラムにおいて、
前記認証情報生成処理で、前記利用者情報と時間情報とチェックデータとから、認証情報を生成し、さらにこの認証情報を暗号化する処理を、
前記情報提供サーバで実行させるためのプログラム。
【請求項２３】請求項２１記載のプログラムにおいて、
前記認証連携処理が、
前記認証情報を復号する処理と、
復号された前記認証情報のチェックデータを検査する処理と、
前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す処理と、
前記時間情報の検査を行う処理と、
を含み、
前記各処理を、前記情報提供サーバで実行させるためのプログラム。
【請求項２４】端末からネットワークを介してアクセスされる情報提供サーバが、
前記端末より送信される、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する手段と、
前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成手段と、
前記生成された認証情報を前記端末に送信する手段と、
を備えている、ことを特徴とする情報提供サーバ装置。
【請求項２５】端末とネットワーク接続され前記端末より送信される利用者情報を受信し、前記利用者情報と時間情報から認証情報を生成し、前記生成した認証情報を前記端末に送信する手段を備えた情報提供サーバ装置と、認証の連携処理を行う情報提供サーバであって、
前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段と、
前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段とを備えている、ことを特徴とする情報提供サーバ装置。
【請求項２６】前記認証連携処理手段が、
前記認証情報を復号する手段と、
復号された前記認証情報のチェックデータを検査する手段と、

前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す手段と、
前記時間情報の検査を行う手段と、
を含み、前記時間情報の検査結果が正しい場合、認証成功とする、ことを特徴とする請求項２４記載の情報提供サーバ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、認証システム及び方法に関し、特にサーバで認証連携処理を行う方法とシステムと装置並びにプログラムに関する。

【０００２】

【従来の技術】利用者認証連携システムとして、例えば特開平１１－３１１２９号公報には、複数のWWW（World Wide Web）サーバを備えたネットワークシステムにおいて、利用者は一度認証すれば、認証有効時間内は、付与された一意の不可視のＩＤをもとに、複数ページや異なるWWWサーバにわたってアクセスを可能としたWWWサーバ連携システムが提案されている。このWWWサーバ連携システムにおいて、セッションＩＤを用いて連携を処理するホストは、複数のいずれかのWWWサーバから通知されたブラウザからＨＴＭＬ（HyperText Markup Language）文書を解析し、セッションＩＤが付与されていなかったときに、ユーザ情報の入力要求を、WWWサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセッションＩＤを生成し、再び、WWWサーバを介してセッションＩＤを埋め込んだＨＴＭＬ文書をブラウザに送信するとともに、有効時間情報を管理し、有効時間情報範囲内のとき、認証を許可する。すなわち、認証が必要な場合、端末によって送信されたＩＤ、パスワードはWWWサーバを経由してホストに送信され、認証が行われる。ホストによって認証が成功した場合、ホストによりセッションＩＤが生成され、そのセッションＩＤは、結果と共にWWWサーバ経由で端末に送られ、利用者からのアクセス時には、端末から送信される要求には、セッションＩＤが自動的に付加されており、そのセッションＩＤはホストによって検証される。

【０００３】しかしながら、この利用者認証連携システムは、次のような問題点を有している。

【０００４】第１の問題点は、ホストが利用できないWWWサーバとは連携ができない、ということである。その理由は、セッションＩＤの検証、生成が、専ら、ホストで行われる、ためである。

【０００５】第２の問題点は、利用者からの要求が増大した場合、そのレスポンスが低下する、ということである。その理由は、すべてのWWWサーバは、すべての利用者からのアクセスごとに、同一のホストに対して、セッションＩＤの検証や生成を要求する構成とされている、ためである。

【０００６】また特開２０００－２２２３６０号公報には、クライアント手段と、認証サーバ手段と、認可サーバ手段を備え、クライアント手段は、認証サーバと、秘密情報を共有し、認証サーバ手段は、秘密情報を不可逆演算ｆをｎ回行った照合情報を含む認証チケットを発行し、クライアント手段は認可サーバに、不可逆演算ｆをｎ－ｋ回行った提示情報を示し、認可サーバは、提示情報に不可逆演算ｆをｋ回行って照合情報と一致するかチェックする認証システム、方法が提案されている。このシステムも、認証サーバ手段と、認可サーバ手段に接続できない、WWWサーバ、端末では、適用できない。また、例えば特開平１０－１７７５５２号公報には、クライアントと複数のサーバ間に認証応答管理部を有する代理サーバを設け、認証応答管理部が、クライアントを認証し、一旦認証したクライアントについて複数のサーバに対する認証情報の応答を代行する認証応答方法と装置が開示されている。

【０００７】

【発明が解決しようとする課題】したがって本発明が解決しようとする課題は、認証を行うサーバを利用できないWWWサーバでも、認証の連携を可能とする方法及びシステムと装置並びにプログラムを提供することにある。

【０００８】

【課題を解決するための手段】前記課題を解決するための手段を提供する本発明に係る方法は、端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから、認証情報を生成し、生成した前記認証情報を、前記端末に送信するステップと、前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行うステップと、を含む。

【０００９】本発明に係る方法は、端末が、利用者からの要求と、利用者認証を行うための利用者情報を、一の情報提供サーバに送信するステップと、前記一の情報提供サーバでは、前記利用者情報を、認証サーバに送信し、前記認証サーバでの認証が成功した場合に、前記一の情報提供サーバの認証情報生成部にて、認証情報を生成するステップと、前記一の情報提供サーバは、前記一の情報提供サーバの前記認証情報生成部で生成された前記認証情報を、要求結果と共に、前記端末に送信するステップと、前記端末が、前記一の情報提供サーバと連携し、認証の連携処理を行う他の情報提供サーバに要求を送信する場合、前記認証情報を、前記他の情報提供サーバを送信するステップと、前記他の情報提供サーバで

は、前記端末から送信された前記認証情報を受け取り、認証連携処理部で、前記認証情報を基に、認証の連携処理を行うステップと、前記他の情報提供サーバにおいて、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信するステップと、を有する。

【００１０】別のアスペクトにおいて、本発明に係るシステムは、端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから、認証情報を生成し、生成した前記認証情報を、前記端末に送信する手段を備え、前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行う手段を備えている。

【００１１】さらに、別のアスペクトにおいて、本発明に係るプログラムは、端末からネットワークを介してアクセスされる一の情報提供サーバが、（ａ）前記端末から利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する処理と、（ｂ）前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成処理と、（ｃ）前記生成された認証情報を、要求結果と共に、前記端末に送信する処理と、を有し、端末からネットワークを介してアクセスされ前記一の情報提供サーバと認証の連携処理を行う情報提供サーバが、（ｄ）前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理と、（ｅ）前記認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する処理とを含み、前記各処理を前記各情報提供サーバで実行させるためのプログラムよりなる。

【００１２】

【発明の実施の形態】本発明の実施の形態について説明する。本発明は、その好ましい一実施の形態において、ブラウザ機能を有する端末(図１の１)から、ＩＰ（Internet Protocol）網等のネットワークを介してアクセスされる情報提供サーバ（WWW（World Wide Web）サーバ）（図１の２）が、端末(図１の１)から入力されＷＷＷサーバ（２）に送信された利用者情報を受け取る手段（図１の２１）と、利用者情報と、前記一のＷＷＷサーバでの時間情報とから、認証情報を生成する手段（図１の２３）と、生成した前記認証情報を、前記端末に送信する手段（図１の２１）を備えている。また端末（図１の１）からネットワークを介してアクセスされ、認証の連携処理を行うＷＷＷサーバ（図１の３）は、端末（図１の１）から送信された認証情報を受け取る手段（図１の３１）と、該認証情報を復号して利用者情報及び時間情報を取り出し、時間検査を行うことで認証判定を行う手段（図１の３４）を備えている。

【００１３】本発明は、その好ましい一実施の形態において、認証サーバ（図１の４）に接続される一のＷＷＷサーバ（図１の２）は、端末（図１の１）が、利用者からの要求と、利用者認証を行うための利用者情報を、ＷＷＷサーバ（図１の２）に送信した場合、これを受信し、前記利用者情報を認証サーバ（図１の４）に送信する手段（図１の２１、２２）と、認証サーバ（図１の４）での認証が成功した場合に、前記利用者の前記利用者情報と時間情報から認証情報を生成する認証情報生成手段（図１の２３）と、前記生成された認証情報を、要求結果と共に、前記端末に送信する手段（図１の２１）と、を備えている。

【００１４】端末（図１の１）は、認証の連携処理を行うＷＷＷサーバ（図１の３）に要求を送信する場合、ＷＷＷサーバ（図１の２）より送信された前記認証情報を、認証の連携処理を行う前記ＷＷＷサーバ（図１の３）に送信する手段（図１の１１）を備えている。

【００１５】認証の連携処理を行うＷＷＷサーバ（図１の３）は、前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段（図１の３４）と、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段（図１の３１）とを備えている。

【００１６】本発明は、その好ましい一実施の形態において、前記一のＷＷＷサーバで生成される認証情報が、利用者情報と時間情報と、チェックデータとを含み、これらの情報が暗号化されている。

【００１７】認証の連携処理を行うＷＷＷサーバ（図１の３）において、認証連携処理手段（図１の３４）は、認証情報を復号する手段（図４のＢ１）と、復号された認証情報のチェックデータを検査する手段（図４のＢ２）と、該チェックデータの検査結果が正しい場合、復号された認証情報から利用者情報と時間情報を取り出す手段（図４のＢ３）と、前記時間情報の検査を行う手段（図４のＢ４）と、を含み、前記時間情報の検査結果が正しい場合、認証成功とする。

【００１８】本発明の別の実施の形態において、上記した認証情報生成手段（図５の２３）を備えたＷＷＷサーバ(図５の５)が、認証連携処理手段（図５の５４）をさらに備えた構成としてもよい。ＷＷＷサーバ(図５の５)は、端末(図５の１)から送信された認証情報を受け取り、認証連携処理手段（図５の５４）で認証連携を行

い、認証判定が成功した場合、認証情報生成手段（図５の５４）に対して認証情報の生成を依頼し、認証情報生成手段（図５の２３）は、認証連携処理手段（図５の５４）が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報から認証情報を生成する。

【００１９】認証の連携処理を行うWWWサーバ（図５の６）が、認証情報生成手段（図５の６３）をさらに備えた構成としてもよい。認証の連携処理を行う前記WWWサーバ（図５の６）が、前記認証連携処理手段（図５の３４）で認証連携を行い、認証判定が成功した場合、認証の連携処理を行うWWWサーバ（図５の６）の前記認証情報生成手段（図５の６３）に認証情報の生成を依頼し、前記認証情報生成手段（図５の６３）が、前記認証連携処理手段（図５の３４）が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報とから認証情報を生成し、利用者の要求結果と認証情報を前記端末に送信する。

【００２０】WWWサーバにおける認証情報生成手段、認証連携処理手段は、WWWサーバのノードコンピュータで実行されるプログラムによりその処理、機能が実現される。

【００２１】複数のWWWサーバが、利用者を認証する場合に、認証処理サーバが共通的に利用できない環境である場合には、WWWサーバが認証処理サーバを利用することなしに、利用者の認証の連携をできるようにしている。

【００２２】図１は、本発明の一実施の形態のシステム構成を示す図である。図１において、端末（１）は、WWWサーバ（２）等にインターネットプロトコル網等のネットワークを介して接続され、端末（１）から入力された認証用の利用者情報は、WWWサーバ（２）を介して認証サーバ（４）に提供される。

【００２３】端末（１）の利用者要求送受信手段（１１）は、利用者からの要求を、WWWサーバ（２）の利用者要求処理手段（２１）に送信する。送信される要求には、初回時には利用者認証を行うための利用者ＩＤ、パスワードなどのような利用者情報が共に送信される。

【００２４】WWWサーバ（２）の利用者要求処理手段（２１）は、利用者情報を認証要求手段（２２）に送信する。認証要求手段（２２）は、認証サーバ（４）の認証処理手段（４１）にその利用者情報を送信し、その利用者が利用可能かの結果を待つ。

【００２５】認証サーバ（４）の認証処理手段（４１）で認証が成功した場合、認証成功という結果がWWWサーバ（２）の認証要求手段（２２）に返され、認証要求手段（２２）は、認証情報生成手段（２３）に、認証情報の生成を依頼する。

【００２６】WWWサーバ（２）の利用者要求処理手段（２１）は、認証情報生成手段（２３）によって生成された認証情報を、その要求結果と共に、端末（１）の利用者要求送受信手段（１１）に送信する。この認証情報には、利用者情報や時間情報が含まれ、利用者が続く要求を送信する場合、利用者要求送受信手段（１１）が自動的に共に送信するようになっている。

【００２７】続いて利用者が、WWWサーバ（２）と連携する第２のWWWサーバ（３）の利用者要求処理手段（３１）に要求を送信した場合、共に、認証情報が送信される。

【００２８】その場合、その認証情報を基に、WWWサーバ（３）の認証連携処理手段（３４）で認証連携処理が行われる。

【００２９】認証連携処理によって、認証情報の正しさが検証され、利用者が認証された場合は、その利用者の要求を受け付けることになるが、WWWサーバ（３）の利用者要求処理手段（３１）は、その要求結果を、端末（１）の利用者要求送受信手段（１１）に送信する。

【００３０】これにより、認証処理サーバを利用することなしに、利用者連携を行うことを可能にする。

【００３１】

【実施例】上記した実施の形態についてさらに具体的かつ詳細に説明すべく本発明の実施例について説明する。図１は、本発明の一実施例のシステム構成の一例を示す図である。図１を参照すると、本発明の一実施例に係るシステムは、利用者が要求を送受信する端末１と、その利用者要求を処理するWWWサーバ２と、WWWサーバ２と連携してその利用者要求を処理する第２のWWWサーバ３と、利用者の認証情報を処理する認証サーバ４とを含む。なお、この実施例において、WWWサーバが提供する情報の内容、種類は問わないが、処理要求の実行にあたり、利用者の認証が必要とされるものとする。

【００３２】端末１は、利用者の要求をWWWサーバに送信し、WWWサーバからの処理結果を受信する利用者要求送受信手段１１を備える。利用者要求送受信手段１１は、要求を送信する際には、WWWサーバ２の認証情報生成手段２３が生成した認証情報がある場合には、該要求と共に自動的に送信する。要求が処理された場合には、WWWサーバ２の利用者要求処理手段２１や、WWWサーバ３の利用者要求処理手段３１から送信される要求結果を受信する。

【００３３】WWWサーバ２は、利用者要求処理手段２１と、認証要求手段２２と、認証情報生成手段２３とを備える。

【００３４】WWWサーバ２において、利用者要求処理手段２１は、利用者要求送受信手段１１から送られてきた要求を処理する。初回要求時には、要求と共に送信されてきた利用者ＩＤ、パスワードのような利用者情報を認証要求手段２２に渡し、認証結果を得る。認証サーバ２での認証が成功し、WWWサーバ２が要求結果を、端末１に送信する際には、認証情報生成手段２３にて生成された認証情報を、要求結果と共に、端末１の利用者要

求送受信手段１１に送信する。

【００３５】WWWサーバ２において、認証要求手段２２は、利用者要求手段２１から渡された利用者情報を、認証サーバ４の認証処理手段４１に送信し、認証サーバ４のから認証結果を受け取る。

【００３６】認証サーバ４で認証が成功した場合には、WWWサーバ２の認証要求手段２２は、認証情報生成手段２３に、認証情報生成を要求する。認証要求手段２２は、認証情報生成手段２３で生成された認証情報を、利用者要求処理手段２１に返す。

【００３７】WWWサーバ２において、認証情報生成手段２３は、認証要求手段２２からの要求に従い、認証情報を生成し、その結果を返す。認証要求手段２２からは利用者情報が渡され、認証情報には、該利用者情報や時間情報が含まれる。

【００３８】第２のWWWサーバ３は、利用者要求処理手段３１と、認証連携処理手段３４を備える。

【００３９】第２のWWWサーバ３において、利用者要求処理手段３１は、利用者要求処理手段２１と同様、利用者要求送受信手段１１から送られてきた要求を処理する。要求と共に送信されてきた認証情報を認証連携処理手段３４に渡し、その結果を得る。認証が成功した場合は、要求結果を利用者要求送受信手段１１に送信する。

【００４０】第２のWWWサーバ３において、認証連携処理手段３４は、利用者要求処理手段３１から渡された認証情報に対し、正しさの検証を行う。利用者情報や時間情報から、認証情報の正しさが確認され、その結果を利用者要求処理手段３１に返す。

【００４１】認証サーバ４は、認証処理手段４１と、利用者管理手段４２とを備える。認証処理手段４１は、認証要求手段２２から利用者情報を受け取る。受け取った利用者情報は、利用者管理手段４２に渡され適合する情報が探される。もし、利用者管理手段４２で適合する情報が見つかった場合には、認証処理手段４１は、「認証成功」の通知を、WWWサーバ２の認証要求手段２２に返す。一方、利用者管理手段４２で適合する情報が見つからなかった場合には、認証処理手段４１は、「認証失敗」の通知を認証要求手段２２に返す。

【００４２】利用者管理手段４２は、認証処理手段４１から渡された利用者情報に対し、保持する管理情報から適合する情報を探し出し、その結果を受け渡す。

【００４３】図２は、本発明の一実施例の動作を説明するためのフローチャートである。図１及び図２を参照して、本発明の一実施例の全体の動作について詳細に説明する。

【００４４】端末１の利用者要求送受信手段１１から利用者の要求が、WWWサーバ２の利用者要求処理手段２１に送信される（図２のステップＡ１およびＡ２）。この場合、利用者情報が送信されるので、利用者要求処理手段２１は、利用者情報を取り出す（図２のステップＡ３）。

【００４５】処理の結果、利用者要求処理手段２１が利用者情報の取り出しに失敗した場合、利用者情報が利用者要求送受信手段１１から正しく送信されてきてないものと判断し、利用者要求処理手段２１は、エラーを、利用者要求送受信手段１１に送信する（図２のステップＡ４）。

【００４６】利用者要求送受信手段１１は、エラーを受信し、その結果は、利用者に対して、端末１の表示装置の画面上に示される（図２のステップＡ５）。図２のステップＡ３において、正しく取り出された利用者情報は、認証要求手段２２に渡され、さらに、認証サーバ４の認証処理手段４１に、認証判定処理が要求される（図２のステップＡ６）。

【００４７】認証サーバ４の認証処理手段４１は、利用者情報を受信する（図２のステップＡ７）。さらに認証処理手段４１は、認証が成功するか調べるため、対象となる利用者情報を利用者管理手段４２に渡し、管理されている情報と適合するか調査を行う（図２のステップＡ８）。この処理は、例えば、コンピュータで行われている、利用者ＩＤとパスワードの検査からなる。処理の結果として、認証が失敗した場合は、その結果が認証要求手段２２に渡され、さらには利用者要求処理手段２１が、エラーを、端末１の利用者要求送受信手段１１に送信する（図２のステップＡ９）。

【００４８】利用者要求送受信手段１１は、エラーを受信し、その結果は、利用者に対し端末１の画面上等に示される（図２のステップＡ１０）。

【００４９】図２のステップＡ８にて、認証判定が成功した場合、認証要求手段２２は、その結果に従い、認証情報生成手段２３に認証情報の生成を依頼する。その際、認証要求手段２２から利用者情報が渡され、認証情報生成手段２３は、受け取った利用者情報や、時間情報から、認証情報を生成する（図２のステップＡ１１）。

【００５０】生成された認証情報は、認証要求手段２２から利用者要求処理手段２１に「認証成功」という結果と共に受け渡される。利用者要求処理手段２１は、利用者の要求結果と認証情報を、利用者要求送受信手段１１に送信し、その結果は、利用者に対して端末１の画面上に示される（図２のステップＡ１２、およびＡ１３）。

【００５１】引き続き、利用者が連携する第２のWWWサーバ３にアクセスするため、利用者要求送受信手段１１から、利用者要求処理手段３１に要求が送信される（図２のステップＡ１４）。第２のWWWサーバ３の利用者要求処理手段３１は該要求を受信し（図２のステップＡ１５）、利用者要求送受信手段１１から該要求と共に自動的に送信された認証情報を取り出す（図２のステップＡ１６）。処理の結果、利用者要求処理手段３１が認証情報の取り出しに失敗した場合、利用者要求処理手段３１は、認証情報が利用者要求送受信手段１１から正

しく送信されてきてないものと判断し、エラーを、端末１の利用者要求送受信手段１１に送信する（図２のステップＡ１７）。端末１の利用者要求送受信手段１１は、エラーを受信し、その結果は、利用者に対し端末１の画面上に示される（図２のステップＡ１８）。

【００５２】図２のステップＡ１６において、第２のＷＷＷサーバ３の利用者要求処理手段３１で正しく取り出された認証情報は、利用者要求処理手段３１から、認証連携処理手段３４に渡される（図２のステップＡ１９）。

【００５３】第２のＷＷＷサーバ３の認証連携処理手段３４は、渡された認証情報に含まれる利用者情報や時間情報から、認証情報の正しさの検証を行う（図２ステップＡ２０）。検証が成功しなかった場合は認証失敗となり、利用者要求処理手段３１は、エラーを端末１の利用者要求送受信手段１１に送信する（図２のステップＡ２１）。

【００５４】利用者要求送受信手段１１は、エラーを受信し、その結果は利用者に対し端末１上に示される（図２のステップＡ２２）。図２のステップＡ２０において、認証判定が成功した場合、認証連携処理手段３４は、利用者要求処理手段３１に認証成功という結果を返す。利用者要求処理手段３１は、利用者の要求結果を、端末１の利用者要求送受信手段１１に送信し、その結果は利用者に対し端末１上に示される（図２のステップＡ２３、およびＡ２４）。

【００５５】次に、図２のステップＡ１１において生成される認証情報について説明する。図３は、生成される認証情報の一例を説明するための図である。図３に示すように、認証情報は、利用者情報や時間情報から成る。利用者情報は、図２のステップＡ１において送信される情報に含まれているものである。時間情報は、図１のＷＷＷサーバ２やＷＷＷサーバ３がシステムとして保持する現在時刻（システムクロックの示す現在の時刻情報；例えば年月日、時刻（時、分、秒）のタイムスタンプ）である。認証情報には、利用者情報や時間情報が組み合わされた情報から生成されるチェックデータが付加され、さらに、暗号化処理が施される。

【００５６】図２のステップＡ２０の認証連携判定処理について説明する。図４は、認証連携判定処理を説明するためのフローチャートである。

【００５７】図４を参照すると、認証連携判定処理は、図３に示す暗号化された認証情報に対して、図４のステップＢ１にて、復号化が行われる。

【００５８】復号化が行われた認証情報に対して、チェックデータの検査が行われる（図４のステップＢ２）。

【００５９】図４のステップＢ２の結果として、チェックデータが異常の場合は、認証連携は失敗となる（図４のステップＢ５）。

【００６０】チェックデータが正常の場合、利用者情報と時間情報が取り出され（図４のステップＢ３）、時間情報が、図１の認証連携処理手段３４に定められている時間内であるか否かの検査が行われる（図４のステップＢ４）。

【００６１】この検査が失敗した場合には、認証連携は失敗と判断され（図４のステップＢ５）、検査が成功した場合には、認証連携成功と判断される（図４のステップＢ６）。

【００６２】上記実施例で説明したＷＷＷサーバ２の利用者要求処理手段２１、認証要求手段２２、及び認証情報生成手段２３、ＷＷＷサーバ３の利用者要求処理手段３１、認証連携処理手段３４の各手段は、ＷＷＷサーバ２、３のコンピュータで実行されるプログラムによりその処理、機能が実現される。

【００６３】次に、本発明の他の実施例について図面を参照して詳細に説明する。図５は、本発明の第２の実施例の構成を示す図である。図５を参照すると、本実施例は、ＷＷＷサーバ５が、図１に示した前記実施例のＷＷＷサーバ２の構成に加え、認証連携処理手段５４を備えている。またＷＷＷサーバ６は、図１に示した前記実施例の第２のＷＷＷサーバ３の構成に加え、認証要求手段６２と認証情報生成手段６３と、を備えている。すなわち、各ＷＷＷサーバは、利用者要求処理手段と、認証要求手段と、認証情報生成手段と、認証連携処理手段を備えている。

【００６４】ＷＷＷサーバ５の認証連携手段５４は、前記実施例における認証連携手段３４と同様に、利用者要求手段２１から渡された認証情報に対して、正しさの検証を行い、さらに、利用者情報や時間情報から、認証情報の正しさが確認され、認証が成功した場合には、認証情報生成手段２３に対して新しい認証情報を要求し、生成されたその認証情報を、利用者要求処理手段２１に返す。

【００６５】ＷＷＷサーバ６の認証要求手段６２は、利用者要求手段３１から渡された利用者情報を、認証処理手段４１に送信し、認証結果を受け取る。認証が成功した場合には、認証情報生成手段６３に対して認証情報生成を要求し、生成されたその認証情報を利用者要求処理手段３１に返す。

【００６６】ＷＷＷサーバ６の認証情報生成手段６３は、認証要求手段６２からの要求に従い、認証情報を生成し、その結果を返す。

【００６７】ＷＷＷサーバ６の認証要求手段６２からは、利用者情報が渡され、認証情報にはその利用者情報や時間情報が含まれる。

【００６８】図６は、本発明の第２の実施例の動作を説明するためのフローチャートである。図６のステップＡ１－Ａ２２で示される、本発明の第２の実施例における利用者要求送受信手段１１、利用者要求処理手段２１、認証要求手段２２、認証情報生成手段２３、認証処理手

段４１および利用者管理手段４２の動作は、図１に示された実施例の各手段１１、２１、２２、２３、４１および４２の動作（図２のステップＡ１－Ａ２２）と同一であるため、その説明は、省略する。

【００６９】前記実施例では、認証連携処理手段３４は、単に、認証情報の正しさのみを確認し、その結果を利用者要求処理手段３１に返していた。

【００７０】この実施例では、図６のステップＡ２０にて、認証判定が成功した場合、WWWサーバ６の認証連携処理手段３４は、認証情報生成手段６３に、認証情報の生成を依頼する。

【００７１】WWWサーバ６の認証情報生成手段６３には、認証連携処理手段３４によって認証情報から得られた利用者情報が渡され、その利用者情報や時間情報から認証情報が生成される（図６のステップＣ１）。生成された認証情報は、認証連携処理手段３４から利用者要求処理手段３１に認証成功という結果と共に受け渡される。

【００７２】WWWサーバ６の利用者要求処理手段３１は、利用者の要求結果と認証情報を、利用者要求送受信手段１１に送信し、その結果は利用者に対し端末１上に示される（図６のステップＡ２３、およびＡ２４）。

【００７３】このようにWWWサーバ６の認証連携処理手段６３によって生成された認証情報が、端末１の利用者要求送受信手段１１に渡されることで、さらなる認証連携処理を行うことができる。

【００７４】次に、図５と図７を参照して、さらなる認証連携処理の動作について説明する。図５において、利用者が端末１からWWWサーバ５にアクセスするため、その要求が、利用者要求送受信手段１１から、WWWサーバ５の利用者要求処理手段２１に送信される（図７のステップＤ１）。

【００７５】WWWサーバ５の利用者要求処理手段２１はその要求を受信し（図７のステップＤ２）、利用者情報を取り出す（図７のステップＤ３）。処理の結果、利用者要求処理手段２１が利用者情報の取り出しに成功した場合、利用者情報を用いた認証連携処理に移行する（図７のステップＤ４）。利用者情報を用いた認証連携処理は、図２のステップＡ６以降の処理と同一であるため、説明は省略する。

【００７６】図７のステップＤ３にて、利用者要求処理手段２１が利用者情報の取り出しに失敗した場合、利用者要求送受信手段１１から要求と共に自動的に送信された認証情報を取り出す（図７のステップＤ５）。

【００７７】処理の結果、利用者要求処理手段２１が認証情報の取り出しに失敗した場合、認証情報が利用者要求送受信手段１１から正しく送信されてきてないと判断し、利用者要求処理手段２１はエラーを利用者要求送受信手段１１に送信する（図７のステップＤ６）。

【００７８】端末１の利用者要求送受信手段１１はエラーを受信し、その結果は利用者に対し端末１上に示される（図７のステップＤ７）。

【００７９】図７のステップＤ５において、正しく取り出された認証情報は、利用者要求処理手段２１から認証連携処理手段５４に渡される（図２のステップＤ８）。認証連携処理手段５４は、渡された認証情報に含まれる利用者情報や時間情報から、認証情報の正しさの検証を行う（図７ステップＤ９）。

【００８０】検証が成功しなかった場合は、認証失敗となり、利用者要求処理手段２１がエラーを利用者要求送受信手段１１に送信する（図７のステップＤ１０）。

【００８１】利用者要求送受信手段１１は、エラーを受信し、その結果は、利用者に対し端末１上に示される（図７のステップＤ１１）。

【００８２】図７のステップＤ９にて認証判定が成功した場合、認証連携処理手段５４は、認証情報生成手段２３に認証情報の生成を依頼する。

【００８３】認証情報生成手段２３には、認証連携処理手段５４によって認証情報から得られた利用者情報が渡され、その利用者情報や時間情報から、認証情報が生成される（図７のステップＤ１２）。

【００８４】生成された認証情報は、認証連携処理手段５４から利用者要求処理手段２１に認証成功という結果と共に受け渡される。

【００８５】利用者要求処理手段２１は、利用者の要求結果と認証情報を、利用者要求送受信手段１１に送信し、その結果は利用者に対し端末１上に示される（図２のステップＤ１３、およびＤ１４）。

【００８６】図７のステップＤ１３に引き続き、図５に示すシステム構成において、利用者がさらにWWWサーバ６にアクセスをする場合、これは、図２のステップＡ１４以降と同様の処理で認証連携を処理することができる。図５に示すシステム構成において、端末１から利用者がさらにWWWサーバ５にアクセスをする場合、これは、図７のステップＤ１以降と同様の処理で認証連携を処理することができる。

【００８７】また、図５に示すシステム構成において、利用者がWWWサーバ６に最初アクセスをする場合でも、図６の各処理においてWWWサーバ５とWWWサーバ６を置き換えれば、同一の動作で処理を行うことができる。

【００８８】この第２の実施例は、すべてのWWWサーバが、認証連携処理手段と認証情報生成手段を持つため、利用者からの要求が複数回続く場合でも、すべてのWWWサーバで認証連携を処理できるという新たな効果を有する。また、さらに認証処理サーバが共通的に利用できる同一構成のWWWサーバから成る分散環境において、利用者からWWWサーバへの最初のアクセスのみに、認証サーバを利用する利用者認証処理が行われ、続くアクセスでは認証連携処理が行われるため、認証処理

サーバへのアクセス回数が少なくなり、利用者の要求へのレスポンス送信時間が短縮できるという新たな効果を有する。

【００８９】

【発明の効果】以上説明したように、本発明によれば、情報提供サーバ（WWWサーバ）間で利用者認証連携をする場合に、すべての情報提供サーバが認証処理サーバを利用できない環境においても、利用者認証ができることである、という効果を奏する。

【００９０】その理由は、本発明においては、認証サーバで利用者情報により認証された後に生成される認証情報が、認証処理サーバを利用できない情報提供サーバの認証連携処理手段によって、認証サーバにアクセスすることなしに、その正当性が確認される、構成としたためである。

【図面の簡単な説明】

【図１】本発明の一実施例のシステム構成を示す図である。

【図２】本発明の一実施例の動作を説明するための流れ図（フローチャート）である。

【図３】本発明の一実施例における認証情報の作成を説明するための図である。

【図４】本発明の一実施例における認証連携処理の動作を説明するための流れ図（フローチャート）である。

【図５】本発明の他の実施例のシステム構成を示す図である。

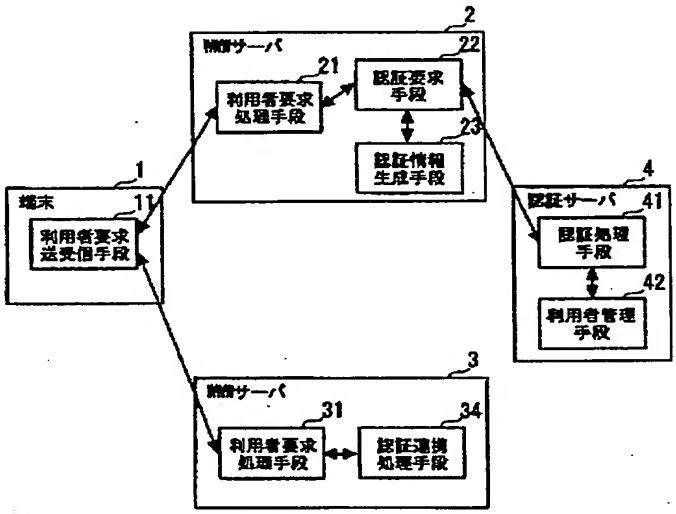
【図６】本発明の他の実施例の動作を説明するための流れ図（フローチャート）である。

【図７】本発明の他の実施例の認証連携処理の動作を説明するための流れ図（フローチャート）である。

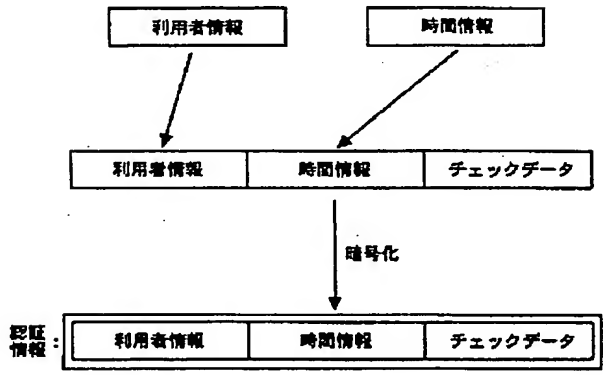
【符号の説明】

１　端末
２、３、５、６　WWWサーバ
４　認証サーバ
１１　利用者要求送受信手段
２１　利用者要求処理手段
２２　認証要求手段
２３、６３　認証情報生成手段
３１　利用者要求処理手段
３４、５４　認証連携処理手段
４１　認証処理手段
４２　利用者情報管理手段

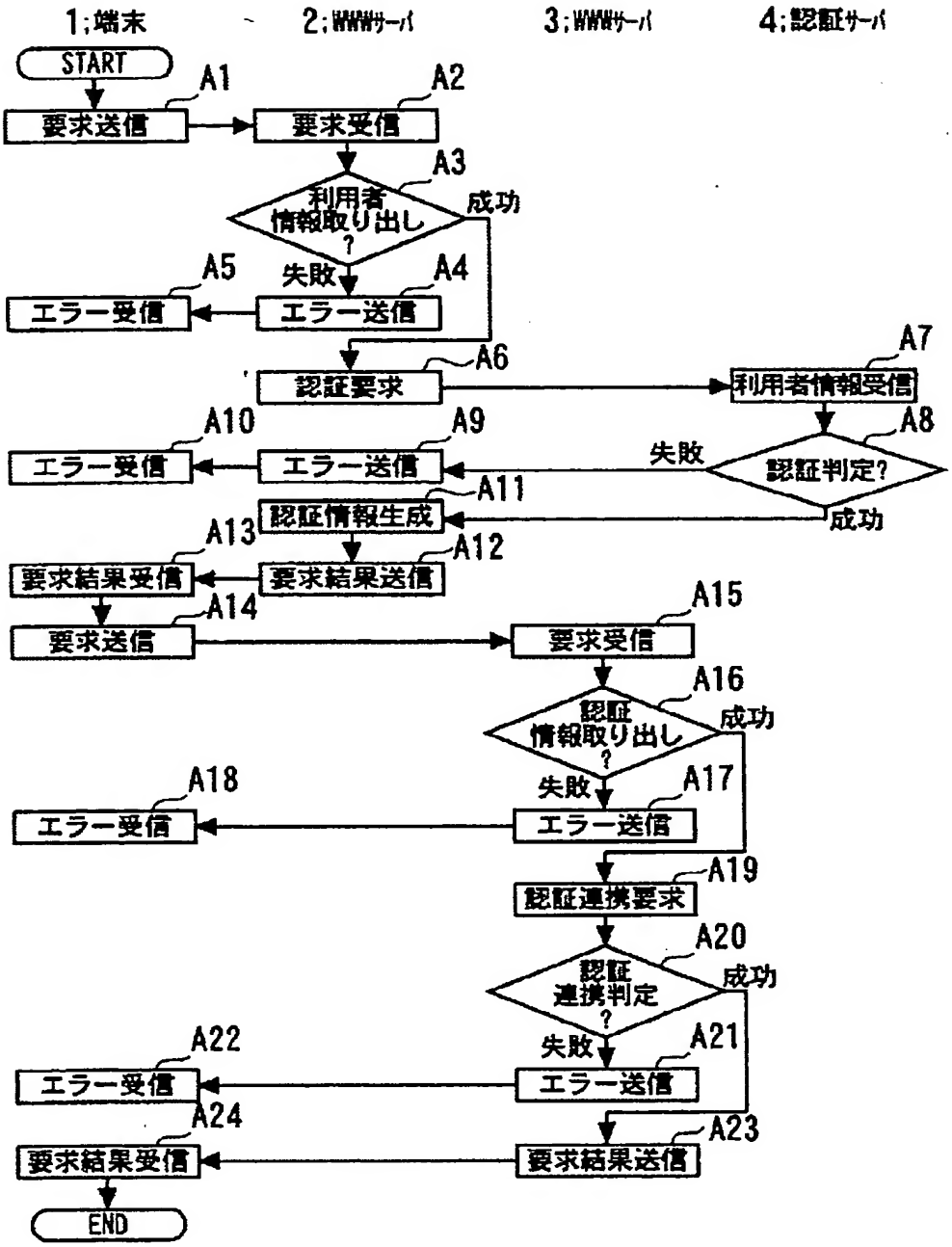
【図１】



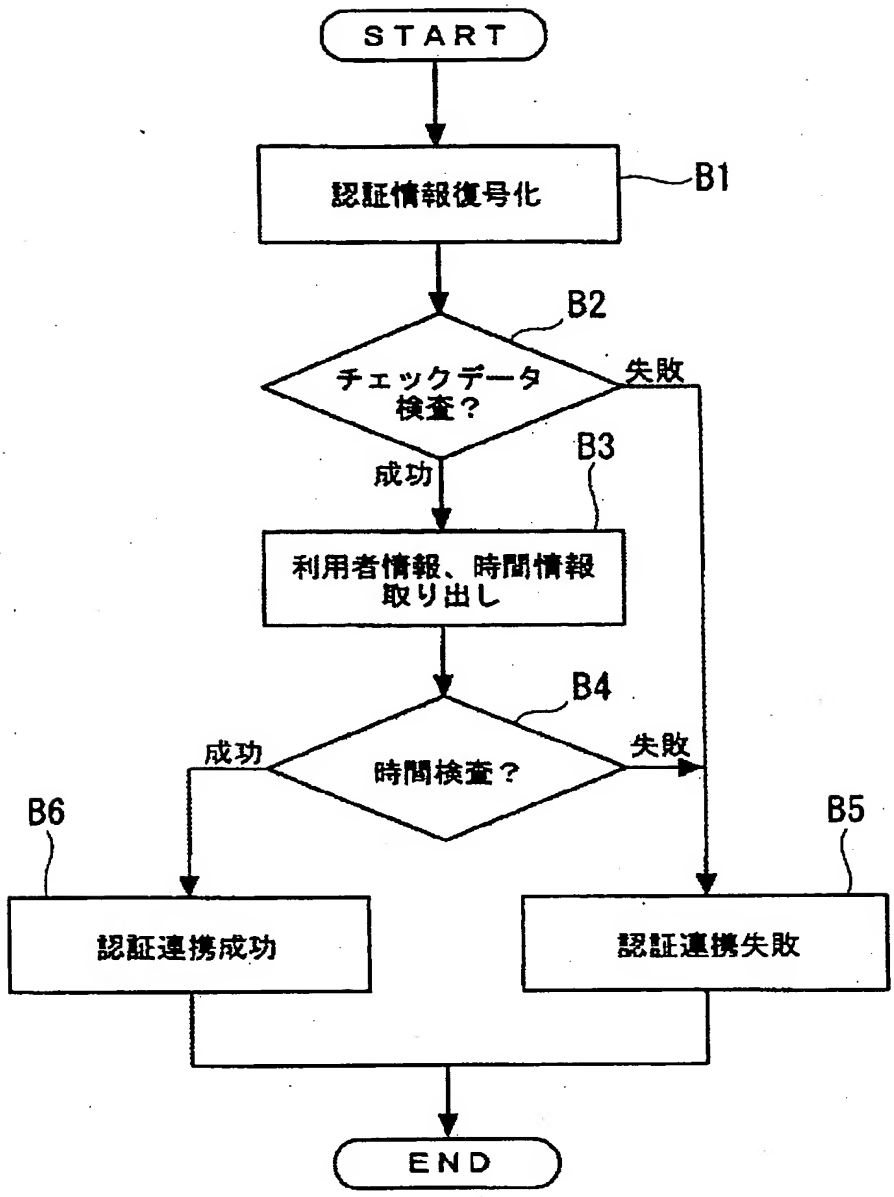
【図３】



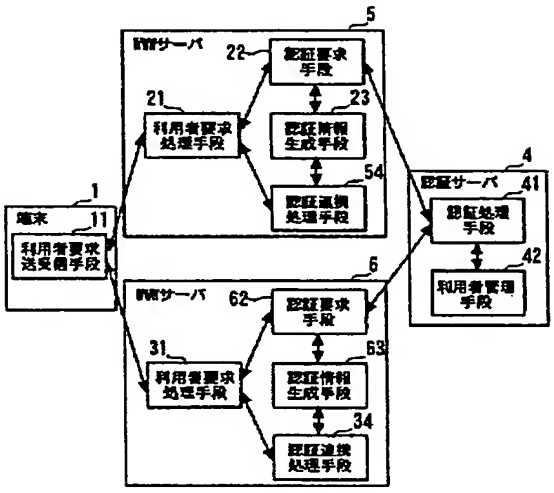
【図２】


1;端末
2;WWWサーバ
3;WWWサーバ
4;認証サーバ
START
A1
要求送信
A2
要求受信
A3
利用者情報取り出し?
成功
失敗
A4
エラー送信
A5
エラー受信
A6
認証要求
A7
利用者情報受信
A8
認証判定?
失敗
成功
A9
エラー送信
A10
エラー受信
A11
認証情報生成
A12
要求結果送信
A13
要求結果受信
A14
要求送信
A15
要求受信
A16
認証情報取り出し?
成功
失敗
A17
エラー送信
A18
エラー受信
A19
認証連携要求
A20
認証連携判定?
成功
失敗
A21
エラー送信
A22
エラー受信
A23
要求結果送信
A24
要求結果受信
END

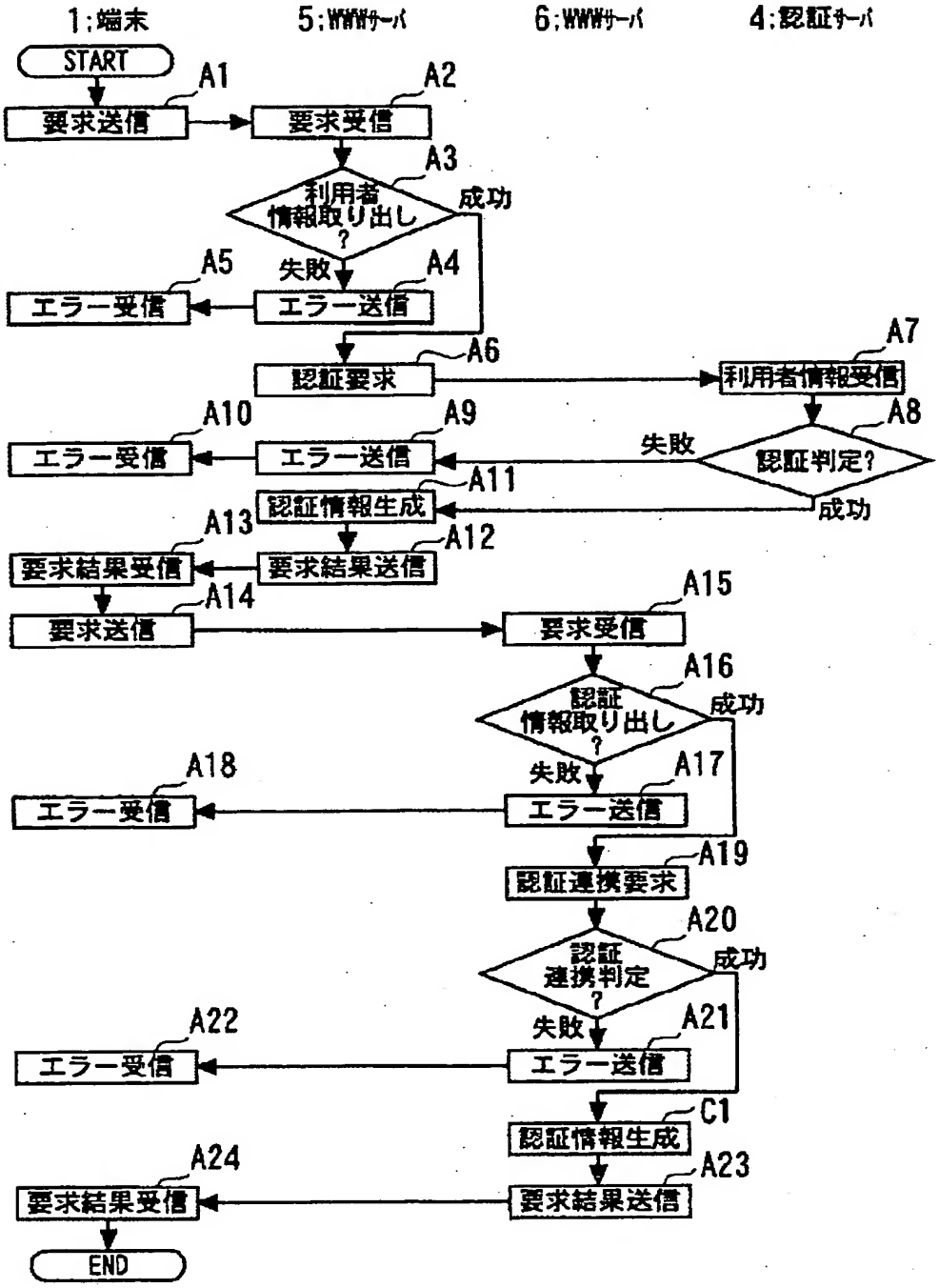
【図４】


START
認証情報復号化
B1
B2
チェックデータ検査？
失敗
成功
B3
利用者情報、時間情報取り出し
B4
時間検査？
成功
失敗
B6
B5
認証連携成功
認証連携失敗
END

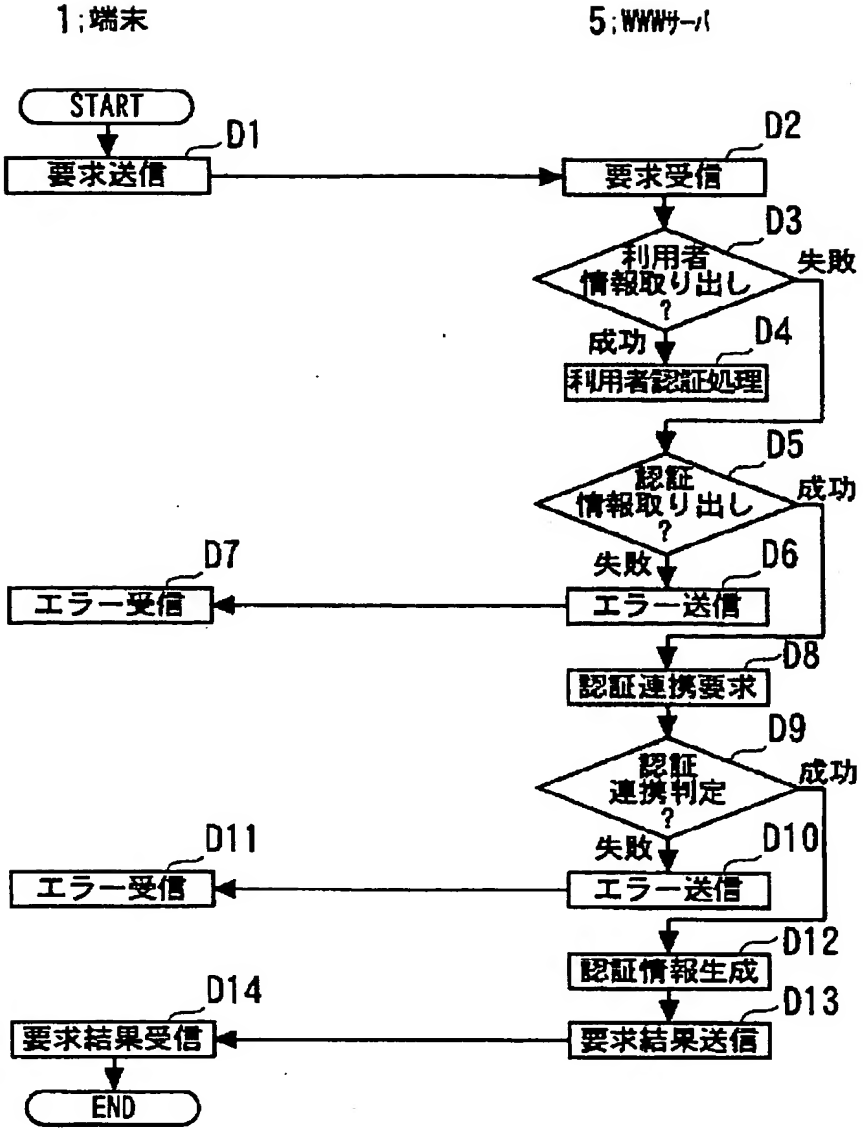
【図５】


5
WWWサーバ
22
認証要求手段
21
利用者要求処理手段
23
認証情報生成手段
54
認証連携処理手段
4
認証サーバ
41
認証処理手段
42
利用者管理手段
1
端末
11
利用者要求送受信手段
6
WWWサーバ
62
認証要求手段
31
利用者要求処理手段
63
認証情報生成手段
34
認証連携処理手段

【図６】


1:端末
5:WWWサーバ
6:WWWサーバ
4:認証サーバ
START
A1
要求送信
A2
要求受信
A3
利用者情報取り出し?
成功
失敗
A4
エラー送信
A5
エラー受信
A6
認証要求
A7
利用者情報受信
A8
認証判定?
失敗
成功
A9
エラー送信
A10
エラー受信
A11
認証情報生成
A12
要求結果送信
A13
要求結果受信
A14
要求送信
A15
要求受信
A16
認証情報取り出し?
成功
失敗
A17
エラー送信
A18
エラー受信
A19
認証連携要求
A20
認証連携判定?
成功
失敗
A21
エラー送信
A22
エラー受信
C1
認証情報生成
A23
要求結果送信
A24
要求結果受信
END

【図７】


1;端末
5;WWWサーバ
START
D1
要求送信
D2
要求受信
D3
利用者情報取り出し?
失敗
成功
D4
利用者認証処理
D5
認証情報取り出し?
成功
失敗
D6
エラー送信
D7
エラー受信
D8
認証連携要求
D9
認証連携判定?
成功
失敗
D10
エラー送信
D11
エラー受信
D12
認証情報生成
D13
要求結果送信
D14
要求結果受信
END